UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

SUSAN B. LONG, DAVID BURNHAM, and TRAC REPORTS, INC. Plaintiffs, v. U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, and U.S. CUSTOMS AND BORDER PROTECTION, Defendants.	Civil Action No.: 5:23-cv-01564 (DNH/TWD)

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT'S MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR SUMMARY JUDGMENT

CARLA B. FREEDMAN
United States Attorney

By: David M. Katz
Assistant United States Attorney
100 South Clinton Street
Syracuse, New York 13202

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

PRELIMINARY STATEMENT

Plaintiffs seek a massive trove of information consisting of thousands of datapoints—including sensitive personal information—about millions of individuals under the Freedom of Information Act ("FOIA"). Plaintiffs ask Immigration and Customs Enforcement ("ICE") to provide data from the Enforcement Integrated Database ("EID") about: (1) any person for whom ICE has established an official case seeking that person's removal from the country; and (2) any person who was apprehended pursuant to an "encounter" with Customs and Border Patrol ("CBP") in or after Fiscal Year 2020.

But disclosing this data "presents extreme risks at an alarming scale" to migrants, their families and associates, witnesses to crimes, government officials, attorneys, and even whole migrant communities: "social exclusion and discrimination, psychological distress, political persecution, and assassination" as well as "retaliation, exploitation, and other abuses." Lynch Decl. ¶ 51, 52. These risks, which could materialize through "gangs, cartels, human smugglers, traffickers, and other criminal entities," include "social exclusion and discrimination, psychological distress, political persecution, and assassination." *Id.*, ¶¶ 51, 52. Moreover, complying with Plaintiffs' request would subject the EID to an increased risk of cyberattacks, which itself presents public safety and law enforcement risks.

Plaintiffs' requests do not trigger any production obligations under FOIA for two reasons. First, ICE had no obligation to comply with Plaintiffs' request because of the undue burden Plaintiffs' request would create. Specifically, because of the vast amount of data Plaintiffs seek, the format in which it is sought, and the source of the data, complying with Plaintiffs' request would require ICE to engage in sophisticated and laborious analysis followed by significant computer coding, which would require approximately 8,360 hours of work.

Second, the information Plaintiffs seek includes information that the FOIA exempts from disclosure because it could reasonably interfere with enforcement proceedings, constitute an unwarranted invasion of personal privacy, and endanger the life and physical safety of individuals. Further, the exempt data is not reasonably segregable from the non-exempt data as a technical and practical matter. As a technical matter, while some fields can be identified as problematic at the outset, it is impractical to segregate all potentially exempt data at the outset of the request or to predict how to protect each individual's identity or sensitive information. As a practical matter, ICE cannot feasibly ensure the subjects' identities can be protected given the vast amount of datapoints disclosed given the ever-evolving technological landscape, which allows bad actors to constantly become better sleuths.

FACTUAL BACKGROUND

By letter dated September 21, 2023 (the "Original Request"), Plaintiffs sought "a copy of each table and field of information stored in the current Enforcement Integrated Database (EID) and the current ICE Integrated Decision Support Database (IIDS)." Katz Decl. Exh. **"A"**. In other words, Plaintiffs sought *a complete copy of all data* from EID and IIDS without any limitations whatsoever. Plaintiffs also sought the "code files, lookup tables, or other records which translate each code into its corresponding meaning" and "for each lookup table, or equivalent, records containing the specific location and identity or identities of the fields in the database where these codes are used." *Id.*

Plaintiffs further sought to dictate the terms of the production by demanding ICE provide copies of the EID and IIDS in a manner that preserves "relational information," which Plaintiffs defined as "any field of information contained in the database used to link tables together within each database (i.e. 'linkage fields')," would be preserved. Katz Decl. Exh. **"A"**. Plaintiffs also directed that, for any "relational information" requiring redaction, ICE must create and provide

"substitute keys or codes to link information among the various tables in the databases." *Id.* Plaintiffs requested disclosure in "a csv, tab-delimited, or similar file format that retains the structure of the underlying data and can therefore readily be read back into a database." *Id.*[1]

I. Plaintiffs' Operative FOIA Request Seeks "All Datapoints . . . Directly Or Indirectly Linked To" Large Numbers Of People From The EID.

On August 1, 2024, during litigation, Plaintiffs narrowed their request (the "Operative FOIA Request").[2] Plaintiffs withdrew their Original Request and now seek three categories of records and data from the EID:

> (1) All datapoints (from any time) that are directly or indirectly linked to a person for whom the Agencies have established an official case seeking that person's removal from the country. [("Part 1")]
>
> (2) All datapoints (from any time) that are directly or indirectly linked to a person who was apprehended pursuant to a CBP "encounter" in or after Fiscal Year 2020, with "encounter" used to mean the same thing that CBP uses it to mean in its Nationwide Encounters Database. [("Part 2")]
>
> (3) All code files, lookup tables, or other records that translate the specific codes used in connection with the datapoints contained in paragraphs (1) and (2) above into their corresponding meaning. [("Part 3")]

Katz Decl. Exh. **"C"**.

---

[1] Plaintiffs also requested various information from CBP. Katz Decl. Exh. **"B"**. Plaintiffs now seek the same information from both components. Katz Decl. Exh. **"C"**.

[2] ICE agreed to accept Plaintiffs' August 1, 2024 letter as the operative FOIA request for the purposes of motion practice in this case. However, ICE reserved its right to object to Plaintiffs' alleged right to limit FOIA requests mid-litigation in any way in any other context.

Plaintiffs still seek to have ICE "preserve[] relational information" in producing EID data. *Id.* However, Plaintiffs will not challenge ICE's "decision to redact any free-format fields" (although they "reserve the right to challenge the *format* of those redactions"). *Id.*

II. The EID Contains 12,000 Potential Fields Of Data For Any Given Record And Data Pertaining To 20,000,000 Migrants.

"The EID is the common database repository for all records created, updated, and accessed by a number of software applications, including several DHS law enforcement and homeland security applications." Gibney Decl. ¶ 12. To that end, the EID contains "information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations." *Id.* The "EID is a transactional database," which "is designed to handle frequent transactions." *Id.*, ¶ 17. The EID is thus structured "to allow efficient access by users for high-speed, real-time operations that involve frequent updates, inserts, and deletions." *Id.*, ¶ 19. As such, it is "not optimized for analytics and reporting." *Id.*

The EID's "records document nearly 20 million migrants' cases and contain more than 12,000 fields of data across roughly 1,000 tables," including personal information (PI) [and] sensitive personal information (SPI)."[3] Lynch Decl. ¶ 5. This information "paint[s] detailed pictures of migrants' lives, whereabouts, families, relationships, health, interactions with law enforcement, and in some cases, criminal history." *Id.*, ¶ 16. It also includes demographic information including by not limited to: "birth year, marital status, occupation, gender, country of origin, country of birth, country of citizenship, weight, height, and hair color." *Id.* Sensitive

[3] "Common types of SPI include health information, race, ethnicity, criminal history, identification as a victim of a crime, sexual orientation, gender identity, political affiliation, and religion." *Id.*

personal demographic information includes "ethnicity, religion, veteran status, gender/sexual identity, and whether the individual is transgender." *Id.* Additionally, personal health information includes "health conditions, medical clearances, pregnancy status, and if a pregnant individual is nursing." *Id.*

More broadly, "[r]ecords even document highly intimate and sensitive information about physical disabilities, amputations, the presence of breast or penile implants, the bodily locations of scars, and moles, and detailed descriptions of tattoos." Lynch Decl. ¶ 16. Moreover, approximately 1.2 million of the 20 million migrants whose data is include in the EID are minors. *Id.*, ¶ 13.

III. Disclosure Of EID Data Would Increase The Risk Of Cyberattacks On The EID.

ICE has designated the EID as a high value asset. Fontaine Decl. ¶¶ 5–7. By definition, this designation means "unauthorized disclosure or loss of control of any element . . . could cause *exceptionally grave harm* to the United States." *Id.*, ¶ 7. The information Plaintiffs request, if disclosed, would be akin to publishing to art thieves the blueprints to an art museum:

> Previously, a judge sitting in the United States District Court for the District of Columbia analogized releasing the EID data structure as presenting cybersecurity risks akin to providing a thief with a map of an art museum. If that thief's map is a current version, which shows or lists where each item currently exists and which exits are currently under surveillance, that map holds greater potential to assist the thief in perpetrating a heist. The map would also show connecting tunnels with other museums significantly reducing research to move laterally through the connected museums.

Id., ¶¶ 30, 31.

"The risks of disclosure here presents cyber risks that include, but are not limited to, an increased likelihood of targeted cyberattacks, increased potential for successful data breaches, and unauthorized access to sensitive information." Fontaine Decl. ¶ 32; *see also id.* at ¶¶ 33–39.

As the Chief Information Security Officer explains, "[d]isclosing this information could reasonably result in increased opportunities for bad actors to attack the EID and associated systems," which would have several consequences. Fontaine Decl. ¶ 11. First, it could allow bad actors to "gain access to personally identifiable information (PII) related to noncitizen subjects of the records, other individuals (such as witnesses to crimes or family members) whose identities are contained in the records, ICE personnel, and others involved in the immigration process." *Id.* Second, it could allow bad actors "greater opportunity to predict law enforcement actions" and "evade law enforcement" or "to commit crimes," including by locking the EID. *Id.* Third, a cyberattack could reasonably risk circumvention of the law insofar as an attack could break the chain of custody of evidence for "sensitive law enforcement data" and the EID more generally "potentially forever." *Id.*, ¶ 21. Fourth, it could "allow bad actors to predict enforcement actions and not only to personally evade law enforcement, but to organize a group effort to break the law and evade law enforcement." *Id.*, ¶ 20.

IV. Individuals Can Be Re-Identified From EID Data.

Because the EID contains a large swath of datapoints (including PI, SPI, and DII) for its various records, the risk that a person can be identified from the EID data remains even after all names and other information that directly identifies an individual (personally identifiable information or PII) are removed. Lynch Decl. ¶ 30 ("Advanced analytic techniques currently allow any technically savvy third party to identify individuals even when direct identifiers have been stripped."). These risks are even more pronounced because even innocuous datapoints can be combined and then compared against "low-cost data broker sites," which can provide "access to the other personal information, including the person's phone number, current and previous home addresses, usernames, email, social media accounts, and the names and contact information of

their family members." *Id.*, ¶¶ 46. Using this information, "a motivated individual could use this information to track down someone and find out where they live in and execute attacks." *Id.*

In one test, "ICE cybersecurity personnel were able to re-identify individuals **stripped of full names and other direct identifiers** in just under an hour – simply by searching local city and state online public arrest records" based on data within EID. Lynch Decl. ¶ 42. Once the information Plaintiffs seek is made public, "gangs, cartels, human smugglers, traffickers, other criminal entities, and even abusive spouses or family members" could all employ re-identification techniques to further their goals against the subjects of the data, which could include retaliation against informants and cooperators, punishment for failed criminal operations, identification of victims (such as trafficking victims) and potential victims, or as a means to weaken rivals. *Id.*, ¶¶ 52, 53.

Cyberattackers are "known to publicly release records containing personally identifiable information (PII) data." Fontaine Decl. ¶ 23. The EID also contains "sensitive noncitizen PII records," pertaining to "witnesses, informants, asylum seekers, crime victims, and other protected individuals," whose privacy should be protected. *Id.*, ¶ 24. In a cyberattack scenario, "[b]ad actors seeking to harm particular people could use that information to locate, harass, harm or kill those vulnerable individuals." *Id.*

Mitigating the risk of re-identification is not a simple process. Lynch Decl. ¶¶ 4–13. The risk of re-identification can only be mitigated by *anonymizing* the data, which requires significant work to ensure that the datapoints produced cannot be used to reconstruct the identity of the subject of the information. *Id.*, ¶ 13. Anonymizing the data would require extensive analysis and sophisticated testing, especially because "Plaintiffs seek to have ICE produce the data with substitute identifiers" and "relational information." *Id.*, ¶ 11.

"Exposing . . . migrants whose cases are managed in the EID to re-identification presents extreme risks at an alarming scale." Lynch Decl. ¶ 51. The "[r]isks posed . . . are complex and varied, ranging from social exclusion and discrimination, psychological distress, political persecution, and assassination." *Id.* These risks could materialize from a wide variety of bad actors, including "gangs, cartels, human smugglers, traffickers, other criminal entities, and even abusive spouses or family members." *Id.*, ¶ 52. Other individuals whose information incidentally appears in the EID likewise face similar risks. *Id.*, ¶¶ 53–70.

STANDARD OF REVIEW

Notably, while an agency's actions in response to a FOIA request are reviewed "de novo," the agency's declarations "are accorded a presumption of good faith." *Carney v. U.S. Dep't of Just.*, 19 F.3d 807, 812 (2d Cir. 1994) (citation omitted); *see also U.S. Dep't of Just. v. Reps. Comm. For Freedom of Press*, 489 U.S. 749, 755 (1989). "On summary judgment in FOIA litigation, affidavits submitted by an agency are accorded a presumption of good faith." *Whitaker v. Dep't of Comm.*, 970 F.3d 200, 208 (2d Cir. 2020) (citations omitted).[4] "[D]eclarations supplying facts indicating that the agency has conducted a thorough search and giving reasonably detailed explanations why any withheld documents fall within an exemption are sufficient to sustain the agency's burden." *Carney* , 19 F.3d at 812. An agency's declarations "will serve to support a motion for summary judgment unless a plaintiff-requester provides evidence of bad faith." *Lane v. Dep't of Just.*, No. 1:02-CV-06555-ENVVVP, 2006 WL 1455459, at *10 (E.D.N.Y. May 22, 2006).

[4] Any claim that ICE and CBP did not comply with FOIA deadlines "does not entitle plaintiff[s] to judgment in [their] favor." *Jacobs v. Fed. Bureau of Prisons*, 725 F. Supp. 2d 85, 89 (D.D.C. 2010).

ARGUMENT

The FOIA represents a legislative attempt "to reach a workable balance between the right of the public to know" about government operations "and the need of the Government" to also protect certain information. *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 152 (1989). The FOIA pairs "broad provisions favoring disclosure . . . with . . . specific exemptions." *Id.* at 153. "As noted by the Supreme Court, under FOIA, 'federal jurisdiction is dependent on a showing that an agency has (1) 'improperly' (2) 'withheld' (3) 'agency records.'" *Grand Cent. P'ship, Inc. v. Cuomo*, 166 F.3d 473, 478 (2d Cir. 1999) (quoting *U.S. Dep't of Justice v. Tax Analysts*, 492 U.S. 136, 142 (1989)). FOIA requests cannot be "so unconstrained as to disrupt the government's daily business." *Grand Cent. P'ship, Inc.*, 166 F.3d at 478. "[I]f a person does not make a valid request, the agency cannot be said to have 'withheld' documents." *Lane*, 2006 WL 1455459, at *11.

I. Compliance With Plaintiffs' FOIA Request Would Unduly Burden ICE Because It Would Require Approximately 8,360 Hours (Over 4 Years) Of Work.

"An agency is justified in denying or seeking clarification of FOIA requests that are so broad that the corresponding search for documents would place an inordinate burden on agency resources." *Van Strum v. U.S. Envrnt'l Prot. Agency*, 972 F.2d 1348 (9th Cir. 1992); *see also Dixon v. U.S. Dep't of Just.*, 279 F. Supp. 3d 1 (D.D.C. 2017) ("Where, as here, an agency's response to a FOIA request calls for an unreasonably burdensome search, the agency need not honor the request."), *aff'd*, No. 17-5223, 2018 WL 4610736 (D.C. Cir. Sept. 10, 2018).

"Courts are entitled to rely upon an agency affidavit for an explanation of why a further search would be 'unduly burdensome' when the affidavit is 'relatively detailed, nonconclusory, and not impugned by evidence in the record of bad faith on the part of the agency.'" *Wolf v. Cent. Intel. Agency*, 569 F. Supp. 2d 1, 9 (D.D.C. 2008) (quoting *McGehee v. Cent. Intel. Agency*, 697 F.2d 1095, 1102 (D.C. Cir. 1983)). In this context, "[c]ourts often look for a detailed explanation

by the agency regarding the time and expense of a proposed search in order to assess its reasonableness." *Id.*

As a general principle, "an agency is not required to reorganize its files in response to a plaintiff's request in the form in which it was made." *Goland v. Cent. Intel. Agency*, 607 F.2d 339, 353 (D.C.Cir. 1978). Indeed, Courts have noted agencies' "practical considerations" in complying with FOIA requests should be given weight "because, although the FOIA regime undoubtedly seeks to directly aid citizens in obtaining Government documents, it also strives to achieve that goal without trampling on the agency's perogative to organize and manage its records in a reasonably efficient manner." *Nat'l Sec. Couns. v. Cent. Intel. Agency*, 898 F. Supp. 2d 233, 275–76 (D.D.C. 2012), *aff'd*, 969 F.3d 406 (D.C. Cir. 2020).

Plaintiffs' request for data from the EID presents an undue burden on ICE. The EID is a sprawling database "containing millions of records which are stored in over 1,000 data tables and over 12,000 unique data fields." Gibney Decl. ¶ 13. Plaintiffs request ICE produce all data ("directly or indirectly linked") from the EID pertaining to two groups of subjects. First, Plaintiffs seek this data for every subject for whom either ICE or CBP has "established an official case seeking that person's removal from the country." Katz Decl. Exh. **"C"**. Plaintiffs seek all data "from any time" that EID houses. *Id.* Second, Plaintiffs seek this data for every subject "who was apprehended pursuant to a Customs and Border Protection (CBP) 'encounter' in or after Fiscal Year 2020, with 'encounter' used to mean the same thing that CBP uses it to mean in its Nationwide Encounters Dataset." *Id.* Even as to this group, Plaintiffs seek data "from any time" that EID houses. *Id.*

The EID is not structured to readily provide the information Plaintiffs seek, especially given their requests for all "directly and indirectly" linked data and to preserve "relational information." This reality leads to undue technical and operational burdens for ICE. ICE estimates the amount of data Plaintiffs seek amounts to 3.75 terabytes, which equates to approximately "1.5 billion pages of printed text." Gibney Decl. ¶ 52. Stacking the hypothetical printout of copy paper, the stack would be 500,000 inches high: roughly equivalent to four Eiffel Towers.

From a technical perspective, the EID is not configured to produce the information Plaintiffs seek, and the EID is not designed to produce the data in the way Plaintiffs seek it. Plaintiffs seek information on a person-by-person basis. But the EID does not store information in a centralized, person-by-person way. To the contrary, "the EID uses a design concept called database normalization, which means EID data is organized into over 1,000 smaller tables of data" disbursed across the database landscape. Gibney Decl. ¶ 20. This design decision allows for *operational efficiency* as opposed to statistical or analytic analysis. *Id.*, ¶ 19.

The EID is designed as a diffuse database. Gibney Decl. ¶¶ 20–30. Once the EID receives data about an event, the data is distributed across various tables in the EID where the various pieces of data are stored. Gibney Decl. ¶ 43. This data is then linked to various other tables and user interfaces directly and indirectly. *Id.*, ¶¶ 43, 44. Because of the EID's design, to comply with Part 1 and Part 2 of Plaintiffs' Operative FOIA Request would require ICE to construct a query in computer code to, in effect, reverse engineer the EID to re-create the data Plaintiffs seek in the form that Plaintiffs seek it.[5] *Id.*, ¶ 41. ICE does not currently have such a query. *Id.*, ¶ 41.

[5] "A database query is a structured request for data from a database" that "specif[ies] what information is to be retrieved from the database and how to join the data together from different tables in the database." *Id.* ¶ 35.

First, ICE would need to determine which fields to search for information, which informs the fields that will be part of the query. Because Plaintiffs seek data that is both directly and indirectly linked to a subject, ICE would need to analyze each directly and indirectly linked field within the EID. A Supervisory Management and Program Analyst within ICE believes "there are approximately 30 direct relationships relative to Part 1" and "there are approximately 130 direct relationships relative to Part 2." Gibney Decl. ¶ 44. To determine how to construct the query based on these relationships, the Supervisory Management and Program Analyst estimates ICE will need to spend two months of employee time (320 hours). *Id.* ICE "does not have any existing documentation that outlines all indirect relationships between the tables in EID." *Id.* ¶ 43. Therefore, ICE would need to "look at each . . . table and attempt to work back to the tables containing" responsive "data using other tables and their . . . relationships." *Id.* This process would take at least twenty-nine months (if not more) of employee time (5,040 hours). *Id.*

Second, ICE would determine which fields would require necessarily line-by-line analysis for redactions so that the fields could be excluded at the outset. "This review would include evaluating each data field to determine which are entered via free-text data entry and would also identify which data fields house data that is exempt from disclosure, including but not limited to personally identifiable information and law enforcement sensitive information (among other types of information that is exempt from disclosure or that could lead to re-identification of an individual)." Gibney Decl. ¶ 46. While the number of fields that must be examined are not known at this time, it would take more than eight and a half months of employee time (1,500 hours) to complete this task assuming 75% of the tables must be analyzed. *Id.*

As to Part 2 of Plaintiffs' Operative FOIA Request, ICE does not currently have the infrastructure set up to conduct an analysis of which events constituted CBP "encounters." Therefore, a special query would have to be "design[ed], develop[ed], and test[ed]." Gibney Decl. ¶ 47. Because of the complex nature of this task, it would take approximately three months of employee time (500 hours) to establish this functionality, all for the purpose of conducting a search on Plaintiffs' behalf. *Id.*

As to Part 3 of Plaintiffs' Operative FOIA Request, "ICE would need to expend additional resources deciding how to search for this information and make production of the information, which may involve producing additional documents or, in its discretion, ICE might decide to provide some or all responsive information in a data release." Gibney Decl. ¶ 48.

Third, ICE would construct complex queries to extract the information from EID. Gibney Decl. ¶ 49. The process for query-building is "using the results of the analysis described above to write code in the SQL programming language." *Id.* Indeed, "The SQL code developed would be very complicated as it would potentially need to join up to 750 tables together using primary and foreign key relationships while isolating specific records due to cardinality constraints." *Id.* ICE would also have to extensively test the query before employing it. *Id.* All in all, this step would take approximately five and a half months of employee time to complete (1,000 hours). *Id.*

Fourth, ICE would run the query on the database. ICE estimates it would take more than a week to run the query. Gibney Decl. ¶ 49. During this time, the EID's operational functionality would be impaired by "longer query times and higher resource consumption" during the process. *Id.*, ¶ 19. As a practical matter, this operational impairment would affect "thousands of ICE officers, agents, and other law enforcement personnel" that use the EID on a daily basis for their respective law enforcement purposes. Fontaine Decl. ¶ 4. Indeed, risks associated with impaired

EID functionality are grave: "[t]he . . . EID database is required to be available 24 hours per day, 7 days per week, 365 days per year." *Id.*, ¶ 7(c). Moreover, "[u]navailability of the system would cause irreparable harm to ICE missions [and] functions . . . such that the catastrophic result would not be able to be repaired or set right again." *Id.*

In total, the search process required here would take approximately 8,360 hours of employee time (and another 40 hours to run the queries and validate the data), which exceeds four years of work for a single employee (before accounting for any leave, vacations, holidays, or other time off). Gibney Decl. ¶ 48. By way of summary, here is the timeline:

Step 1	Determining Fields To Search: 5,360 Hours
Step 2	Determining Which Fields To Exclude: 1,500 Hours
Step 2a	For Part 2, Design/Develop/Test Special Functionality; 500 hours
Step 2b	For Part 3, Create Code-Lookup Functionality
Step 3	Build Queries: 1,000 Hours
Step 4	Run Queries, Validate Data
Total	**8,360 Hours; 4+ Years**

Moreover, even this massive estimate may be an underestimation because "fulfillment of these requests would be significantly more complex than any other data extract ever performed by" ICE. Gibney Decl. ¶ 51. Because "undertaking a project of this magnitude would come with significant risk," ICE believes "[i]t is highly likely that unexpected challenges would arise—such as changes in requirements (or changes in our interpretation of the requirements), resource availability, or technical difficulties—that could significantly impact the amount of time to complete" the tasks outlined above. *Id.*

II. FOIA Precludes Compliance With Plaintiffs' Request Because It Seeks Information That Is Incurably Exempt And Not Reasonably Segregable.

FOIA exempts nine categories of otherwise obtainable records from the reach of a FOIA request. 5 U.S.C. § 552(b)(6). Plaintiffs' FOIA request implicates EID data within the ambit of exemptions 3, 6, and 7(a), (c), (e), and (f). While FOIA generally requires disclosure of non-exempt information, this requirement does not apply where, as here, the exempt information is not "***reasonably*** segregable" from the non-exempt information. 5 U.S.C. § 552(b). Indeed, because of the many facets of privacy concerns and the various types of data in the database at issue here, the exempt data cannot be reasonably segregated either at the outset before the search or after the search has been conducted through redactions.[6]

[6] Specific portions of the EID data may qualify for further exemptions. ICE relies on these exemptions specifically both because ICE anticipates the exemptions implicate large swaths of the data sought and because ICE has identified these exemptions as precluding reasonable segregation. In the event further motion practice is ordered or a search must be conducted, ICE reserves its right to rely on other exemptions if ICE ultimately is ordered to perform a search.

A. The EID Data is Exempt from Disclosure Under FOIA Exemption 7: Records And Information Compiled For Law Enforcement Purposes.

Under exemption 7, an agency need not disclose "records or information compiled for law enforcement purposes" in 6 situations. 5 U.S.C. § 552(b)(7). This exemption is not limited to investigatory materials. *Tax Analysts v. Internal Revenue Serv.*, 294 F.3d 71, 79 (D.C. Cir. 2002). Specifically, and as relevant here, FOIA does not require disclosure of such records or information where it:

> (A) "could reasonably be expected to interfere with enforcement proceedings,"
>
> . . . .
>
> (C) "could reasonably be expected to constitute an unwarranted invasion of personal privacy,"
>
> . . . .
>
> (E) "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law," or
>
> (F) "could reasonably be expected to endanger the life or physical safety of any individual."

5 U.S.C. § 552(b)(7)(A), (C), (E) and (F).

The records Plaintiffs seek are undoubtedly "compiled for law enforcement purposes." Notably, this phrase is not limited to the enforcement of criminal statutes. To the contrary, its scope includes civil and administrative statutes. *Pub. Emps. for Env't Resp. v. U.S. Sec'y. Int'l Boundary & Water Comm'n*, 740 F.3d 195, 203–04 (D.C. Cir. 2014) (civil); *Rugiero v. Dep't of Just.*, 257 F.3d 534, 550 (6th Cir. 2001) (same); *Jefferson v. Dep't of Just.*, 284 F.3d 172, 178 (D.C. Cir. 2002) (administrative); *Schiller v. Immig. & Naturalization Serv.*, 205 F. Supp. 2d 648, 659 (W.D. Tex. 2002) (same). Indeed, courts have found that records identifying database tables in ICE's EID

and describing fields of information stored in such tables, and database schema qualified under this threshold. *Long v. Immig. & Customs Enforcement*, 464 F.Supp.3d 409, 419–23 (D.D.C. 2020). CBP records pertaining to passengers also meet the standard. *Concepcion v. U.S. Customs & Border Prot.*, 907 F. Supp. 2d 133, 140–41 (D.D.C. 2012) (explaining that passenger activity reports compiled as part of agency's mission to secure borders of U.S. by collecting and reviewing travel information satisfies law enforcement threshold), *aff'd per curiam*, 550 F. App'x 1 (D.C. Cir. 2013).

i. Exemption 7(A) Applies Because Disclosure Of All EID Data Pertaining To A Person Could Reasonably Interfere With Enforcement Proceedings.

A FOIA request triggers exemption 7(A) when the data sought "*could reasonably* be expected to interfere with enforcement proceedings." 5 U.S.C. § 552(b)(7)(C) (emphasis added); *Citizens for Resp. & Ethics in Wash. v. Dep't of Just.*, 658 F. Supp. 2d 217, 225 (D.D.C. 2009). To invoke exemption 7(A), an agency must establish there is a "pending or reasonably anticipated" proceeding and that there will be a harm to the proceeding. *Juarez v. Dep't of Just.*, 518 F.3d 54, 58–59 (D.C. Cir. 2008). Courts have applied deference to agencies in this analysis, especially where potential national security issues are at play. *Ctr. for Nat. Sec. Stud. v. Dep't of Just.*, 331 F.3d 918, 926 (D.C. Cir. 2003); *Am.-Arab Anti-Discrimination Comm. v. Dep't of Homeland Sec.*, 516 F. Supp. 2d 83, 89 (D.D.C. 2007). Plaintiffs seek information "from any time" for people who have "an official case seeking that person's removal from the country" and/or "who was apprehended pursuant to a CBP 'encounter' in or after Fiscal Year 2020 . . . ." Both requests implicate exemption 7(A).[7]

[7] Additionally, 5 U.S.C. § 552(c)(1) allows an agency to "treat . . . records as not subject to the requirements of" FOIA "[w]henever a request is made which involves access to records described

As to the first prong, both of Plaintiffs' requests implicate enforcement proceedings. Plaintiffs' first request explicitly pertains to "case[s] seeking that person's removal from the country." To the extent any data pertains to pending removal proceedings, it triggers the first prong. Plaintiffs' second request seeks records pertaining to "encounters," which likewise is reasonably likely to implicate enforcement proceedings. *Mapother v. Dep't of Just.*, 3 F.3d 1533, 1542 (D.C. Cir. 1993). Indeed, a likelihood of prospective proceedings is sufficient to trigger this exemption. *Ctr. for Nat. Sec. Stud.*, 331 F.3d at 926; *see also Vento v. Internal Rev. Serv.*, No. 08-159, 2010 WL 1375279, at *7 (D.V.I. Mar. 31, 2010) (finding exemption applies where agency was "preparing a case").

As to the second prong, the agency "is not required to make a specific factual showing with respect to each withheld document that disclosure would actually interfere with a particular enforcement proceeding." *Lazardis v. Dep't of State*, 934 F. Supp. 2d 21, 37 (D.D.C. 2013) (citations omitted). Instead, federal courts may make generic determinations that disclosure of certain kind of records would generally interfere with enforcement proceedings." *Id.* (citations omitted).

Indeed, as to Part 1 of Plaintiffs' request, releasing demographic information regarding those who are subject to removal proceedings could "indirectly reveals the methodologies and data used to make" decisions and could lead to risks of intimidation. *ACLU of Mich. v. Fed'l Bureau of Investig.*, 734 F.3d 460, 466 (6th Cir. 2013); *Ctr. for Nat'l Sec. Stud.*, 331 F.3d at 929. Notably,

---

in subsection (b)(7)(A) to the extent "the investigation or proceeding involves a possible violation of criminal law" and "there is reason to believe that (i) the subject of the investigation or proceeding is not aware of its pendency, and (ii) disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings." Part 2 of Plaintiffs' request likely also contains information that would fall under this exception to FOIA.

as to Part 2 of Plaintiffs' request, information regarding those who have been encountered by CBP could well "reveal much about the focus and scope" of investigations and proceedings. *See Swan v. Secs. & Exch. Comm'n*, 96 F.3d 498, 500 (D.C. Cir. 1996). Moreover, the information together could be used to cause harm on a broader level and give "a composite picture" of CBP encounters and ICE removal proceedings. *Ctr. for Nat'l Sec. Stud.*, 331 F.3d at 928; *Elec. Priv. Info. Ctr. v. Dep't of Just.*, 490 F. Supp. 3d 246, 270 (D.D.C. 2020); *N.Y. Times Co. v. Fed'l Bureau of Investig.*, 297 F. Supp. 3d 435, 446–47 (S.D.N.Y. 2017).

Here, complying with Plaintiffs' FOIA request would increase the risk of a cyberattack on the EID, which in turn could impede enforcement proceedings. First, ICE could be hampered in presenting evidence in its enforcement proceedings. A cyberattack could break the chain of custody of evidence for "sensitive law enforcement data" and the EID more generally "forever." Fontaine Decl. ¶ 21. In that event, the data contained in the EID could be rendered "inadmissible in court," which could impede ICE's "law enforcement mission" because "ICE could be placed in a position where it cannot present reliable or valid data to support the enforcement actions taken." *Id.*

Second, ICE may be impeded in its efforts to secure witnesses' testimony if those witnesses are re-identified. Disclosure of the EID data would involve "highly sensitive" personal information, including "detailed physical descriptions (height, weight, race, complexion), . . . sexual identity/gender, and country of citizenship" as well as "whether the witness has information that may be relevant to federal investigations or if they may be called upon to testify in official court proceedings." Lynch Decl. ¶ 23. This could expose witnesses to bad actors, who might seek

to dissuade witnesses from testifying. *Id.*, ¶ 55.[8]

Third, prosecutors could also be identified by bad actors in an attempt to impede proceedings. Lynch Decl. ¶ 69. Specifically, "[a]ttorneys involved in prosecuting criminal cases involving migrants are particularly at risk of attacks by criminal actors." *Id.* Prosecutors could be targeted—even before indictments or after the conclusion of cases—as a form of intimidation or retribution. *Id.*

ii. Exemption 7(C) Applies Because Disclosing EID Data Could Reasonably Be Expected To Constitute An Unwarranted Invasion Of Personal Privacy.

A FOIA request triggers exemption 7(C) when the data sought "*could reasonably* be expected to constitute *an unwarranted* invasion of personal privacy." 5 U.S.C. § 552(b)(7)(C) (emphasis added); *Nat'l Archives & Recs. Admin. v. Favish*, 541 U.S. 157, 165–66 (2004). Thus, the "government need not prove to a certainty that release will lead to an unwarranted invasion of personal privacy" to invoke this exemption. *Keys v. Dep't of Just.*, 830 F.2d 337, 346 (D.C. Cir. 1987).

Courts employ a balancing test to determine if exemption 7(C) has been triggered. First, an agency must establish that a privacy interest exists in the records or information requested. *Assoc. Press v. Dep't of Def.*, 554 F.3d 274, 284 (2d Cir. 2009). The privacy interest involved in this exemption can relate to the subject of the record as well as any person whose information is contained in the record. *Gabel v. Internal Rev. Serv.*, 134 F.3d 377 (9th Cir. 1998). Likewise, a foreign national's privacy interests are protected by this exemption. *Graff v. Fed'l Bureau of Invest.*, 822 F. Supp. 2d 23, 34 (D.D.C. 2011); *Tuffly v. Dep't of Homeland Sec.*, 870 F.3d 1086,

[8] Indeed, these records could also reasonably be expected to disclose the identity of a confidential source and would also be exempt under Exemption 7(D). 5 U.S.C. § 552(b)(7)(D).

1094 (9th Cir. 2017). Government personnel also have cognizable privacy interests under this exemption. *Fabiano v. McIntyre*, 146 F. App'x 549, 550 (3d Cir. 2005); *Rojas-Vega v. U.S. Citizenship & Immig. Serv.*, 132 F. Supp. 3d 11, 20 (D.D.C. 2015).

Second, the requester must establish a cognizable public interest in disclosure. *Favish*, 541 U.S. at 172; *Lewis v. Dep't of Just.*, 867 F. Supp. 2d 1, 19 (D.D.C. 2011). The requester must establish (1) there is a "significant" public interest in disclosure, and (2) disclosure "is likely to advance that interest." *Id.* The public interest the requester claims must tie into FOIA's purpose. *Reps. Comm. for Freedom of the Press*, 489 U.S. at 773.

Third, and assuming the parties have both offered cognizable interests, the Court must weigh the competing interests to determine whether requester's interest outweighs the privacy interests presented. *Assoc. Press*, 554 F.3d at 284–91; *Adamowicz v. Internal Rev. Serv.*, 552 F. Supp. 2d 355, 369–70 (S.D.N.Y. 2008). Courts are loathe to discount established privacy interests. *Halpern v. Fed'l Bureau of Invest.*, 181 F.3d 279, 297 (2d Cir. 1999); *Reps. Comm. For Freedom of the Press*, 489 U.S. at 770–71. Courts analyze the nature and extent of the privacy interest that would be invaded if the agency is compelled to produce the information. *Assoc. Press*, 554 F.3d at 284. Moreover, privacy interests remain even where other information may allow the public to "piece together" an individual's identity. *Weisberg v. Dep't of Just.*, 745 F.2d 1476, 1491 (D.C. Cir. 1984). Courts also employ a categorical approach to privacy interests if possible. *Reps. Comm. For Freedom of the Press*, 489 U.S. at 776–80. Notably, identities contained in law enforcement records are categorically protected. *See SafeCard Servs., Inc. v. Secs. Enforcement Comm'n*, 926 F.2d 1197, 1206 (D.C. Cir. 1991).

Here, the declarations submitted in support of this motion plainly establish compelling privacy interests across several groups of individuals who could be re-identified if the information is disclosed. The EID contains "approximately 12,000 data fields" pertaining to a migrant and the "migrant's case, including personally information (PI) [and] sensitive personal information (SPI)." Lynch Decl. ¶ 5. SPI includes, for example, transgender identity, ethnicity, health information, highly-specific codes regarding crimes, and other indicators of special vulnerability. *Id.*, ¶ 54. Of particular note, the SPI available from EID data "could result in discrimination or impact the individual's rights, safety, opportunities, and social or psychological well-being." *Id.*, ¶ 7. For example, an individual who is identified from EID data could be publicly identified as transgender, which is sensitive in itself. *Id.* Or, an individual who is identified from EID data could be publicly identified "as a victim of rape." *Id.*

But EID data also contains sensitive information regarding many individuals who are not themselves migrants. Five groups illustrate the breadth of the EID data's reach. First, EID contains highly sensitive personal information regarding witnesses. Lynch Decl. ¶ 23. Second, the EID also contains "detailed information about a migrant's family members and points of contacts." *Id.*, ¶ 24. Third, the EID contains "information about ICE, CBP, USCIS, and other DHS personnel, other government employees and law enforcement agents, and government contractors." *Id.*, ¶ 25. Fourth, and more generally, the EID contains "government officials engaging a migrant's case that access the EID data." and "law enforcement agents." *Id.*, ¶¶ 26–27. Fifth, "[t]he EID also contains information about attorneys representing and prosecuting a migrant's case." *Id.*, ¶ 26. These groups all have unique privacy interests, but common risks of exposing private—including sensitive and/or intimate—information emerge: "social exclusion and discrimination, psychological distress, political persecution, and assassination" as well as "retaliation,

exploitation, and other abuses." *E.g.*, *id.*, ¶¶ 51, 52; *see also id.* at ¶¶ 53–70. Here is just one example of how re-identified EID data could reasonably be expected to invade the privacy of an individual by exposing sensitive information:

> Imagine, for example, that the EID captures an adult male suspected of incest and sodomy against a boy (per the case records' NCIC codes). That individual is also marked as a member of a unique family unit, including a male son whose case is also managed in the EID. The child is thus linked as the son of a parent who is suspected of child sexual abuse. Even without a family unit id, however, Entity Resolution techniques could easily match individuals to their family unit. If EID data is exposed, this child could be accurately identified as a victim of incest, but also falsely identified (e.g. perhaps the actual victim is the adult male's nephew). Either scenario could result in severe emotional and psychological harms, bullying and social exclusion, or even retaliation by the male adult abuser.

Id., ¶ 59.

Panning out, migrant communities also bear risks associated with the release of a broad set of EID data. For example, "EID data can be analyzed to pinpoint clusters of migrant communities that share demographic characteristics." Lynch Decl. ¶ 61. This information could be used by anti-immigrant groups to "harass, attack, or carry out acts of domestic terrorism against a community of migrants belonging to a particular country of origin." *Id.* Or, the information could be used by "[m]embers of one ethnic group [to] identify and target communities they have historical ethnic conflict with." *Id.* Additionally, "[t]raffickers could identify groups of migrants of a particular sex, age, language group, etc. to recruit into various forms of labor exploitation." *Id.* Likewise, "[m]alicious actors could abuse EID data to identify facilities or towns where pockets of minors reside, including clusters of unaccompanied migrant children and children of a particular sex, age, country of origin, ethnicity, or gang-affiliation." *Id.*, ¶ 63.

Moreover, the information pertaining to government officials could be used "for a range of malicious purposes" including "retribution against law enforcement agents who disrupted criminal enterprises" and to "conduct[] counter-surveillance against agents investigating criminal networks." Lynch Decl. ¶ 63. Government officials could likewise be "targeted by a range of pro- and anti-immigration actors" or "doxed." *Id.*, ¶¶ 66, 68. Prosecutors "are particularly at risk of attacks by criminal actors." *Id.*, ¶ 67. Indeed, bad actors could target prosecutors to seek retribution. *Id.*

iii. Exemption 7(E) Applies Because Disclosing The EID Data Would Subject ICE To A Greater Risk Of Cyberattacks, Disclose Law Enforcement Techniques And Procedures, And Could Reasonably Be Expected To Risk Circumvention Of The Law.

Exemption 7(E) protects against disclosure of information that pertains to techniques and procedures for law enforcement investigations and prosecutions. Under this exemption, agencies can protect database information which, if disclosed, would undermine law enforcement efforts. *Blackwell v. Fed'l Bureau of Investig.*, 646 F.3d 37, 42 (D.C. Cir. 2011). Additionally, this exemption provides a mechanism to protect agencies against disclosures that could result in a greater risk of a cyberattack. *Sharkey v. Dep't of Just.*, No. 16-2672, 2018 WL 838678, at * 8 (N.D. Ohio Feb. 13, 2018). Indeed, Plaintiffs and Defendant ICE have previously addressed this issue in the context of metadata within ICE databases. *Long v. Immig. & Customs Enforcement*, 464 F. Supp. 3d 409, 422–23 (D.D.C. 2020). In that case, the Court found it persuasive that disclosure would "incentivize future attacks and make those attacks more harmful" if disclosure was ordered. *Id.*

Here, ICE's Chief Information Security Officer opined, "[d]isclosure of these records would reasonably result in increased opportunities for bad actors to attack EID and associated systems," which would allow bad actors "greater opportunity to predict law enforcement actions" and "evade law enforcement" or "to commit crimes." Fontaine Decl. ¶ 11. Indeed, "[a] cyberattack on EID could lock the database . . . which would impact ICE's ability to identify, arrest and detain individuals who are terrorists, national security threats [and] threats to public safety." *Id.*, ¶ 20. Moreover, in the event of an attack rendering the EID inaccessible, "[o]fficers would be unable to use the database to determine an encountered individual's criminal history, fingerprints and other biometrics, and other factors essential to understanding the threat that individual may represent to the public," which in turn "could reasonably result in ICE officers being required to release dangerous individuals who would otherwise be arrested." *Id.*

Long term, a cyberattack could reasonably risk circumvention of the law insofar as an attack could break the chain of custody of evidence for "sensitive law enforcement data" and the EID more generally "forever." Fontaine Decl. ¶ 21. If this occurs, data contained in the EID may be rendered "inadmissible in court," which could cause circumvention of the law. *Id.* "If data in the database remained inadmissible, ICE's ability to conduct its law enforcement mission . . . would become almost nonexistent" because "ICE could be placed in a position where it cannot present reliable or valid data to support the enforcement actions taken" during the execution of its law-enforcement mission. *Id.* Additionally, EID records contain "records related to law enforcement techniques and procedures" that could be "released to the public" in a cyberattack, which "would allow the reasonably foreseeable harm that the information would be used to commit illegal acts and evade law enforcement." *Id.*, ¶ 22. Therefore, disclosure "would allow bad actors to predict enforcement actions and not only to personally evade law enforcement, but to organize

a group effort to break the law and evade law enforcement." *Id.*

The risk of impeding investigations and prosecutions does not end with the data pertaining to the subjects of the investigations or prosecutions. As to witnesses, disclosure of EID data would involve highly sensitive personal information, including "detailed physical descriptions" and other potentially indirectly identifying information. Lynch Decl. ¶ 23. Additionally, the EID data contains information regarding "whether the witness has information that may be relevant to federal investigations or if they may be called upon to testify in official court proceedings, which . . . may not be known to the subject or other interested parties" absent disclosure in this context. Lynch Decl. ¶ 23. The threats to witnesses principally include the risk of retaliation by "highly organized and violent cartels, human traffickers, and smugglers." *Id.*, ¶ 55. The EID also contains "detailed information about a migrant's family members and points of contacts." *Id.*, ¶ 24. Criminal actors pose risks to the family members of migrants, who may be able to be more easily reached by the criminal organization. *Id.*, ¶ 55. Indeed, criminal actors could reasonably seek to seek retribution or retaliation against family members or "carry out threats against family members to assert control over a migrant." *Id.*, ¶ 55.

As explained above, complying with Plaintiffs' FOIA request would increase the risk of a cyberattack on the EID, which could also risk circumvention of the law. Specifically, a bad actor "could lock the database . . . and all the data within the database, or otherwise make it inaccessible." Fontaine Decl. ¶ 20. This type of attack could risk circumvention of the law by allowing individuals to evade arrest and detention insofar as it would "impact ICE's ability to identify, arrest and detain individuals who are terrorists, national security threats [and] threats to public safety." *Id.* Moreover, "[o]fficers would be unable to use the [EID] to determine . . . the threat that individual may represent to the public," which in turn "could reasonably result in ICE officers being required

to release dangerous individuals who would otherwise be arrested." *Id.*

Relatedly, as to Part 3 of the Operative FOIA Request, Plaintiffs have previously obtained discrete portions of EID data. Fontaine Decl. ¶¶ 26–27. Comparing various versions of the EID can expose law enforcement techniques and procedures because "as law enforcement techniques and procedures evolve, the [EID] must evolve alongside those changes." *Id.*, ¶ 28. Therefore, tracking the database changes is a way of tracking the evolution of law enforcement techniques. *Id.* Indeed, disclosing the current EID database could reasonably expose "the latest and least publicly known techniques and procedures . . . which would allow bad actors to anticipate law enforcement actions, to commit crimes, and to evade law enforcement." *Id.*

iv. Exemption 7(F) Applies Because Disclosing The EID Data Could Reasonably Be Expected To Endanger The Life And Physical Safety Of Several Classes Of Individuals.

Exemption 7(F) protects "records or information compiled for law enforcement purposes" where disclosure "could reasonably be expected to endanger the life or physical safety of any individual." 5 U.S.C. § 552(b)(7)(C); *Pub. Emps. for Envt'l Resp.*, 740 F.3d at 206. This exemption protects "any individual whose life or physical safety" may be at risk. *Amuso v. Dep't of Just.*, 600 F. Supp. 2d 78, 101 (D.D.C. 2009). For example, this exemption protects individuals where disclosure could "likely result in harassment and/or retaliation" if the information is disclosed. *Anderson v. Bureau of Prisons*, 806 F. Supp. 2d 121, 128 (D.D.C. 2011); *Peter S. Herrick's Customs & Int'l Trade Newsl. v. U.S. Customs & Border Prot.*, No. 04-00377, 2006 WL 1826185, at *9 (D.D.C. June 30, 2006).

Notably, unlike exemptions 7(A) and 7(C), for the purposes of exemption 7(F) the agency prevails once it establishes the risks involved in disclosure. *Raulerson v. Ashcroft*, 271 F. Supp. 2d 17, 29 (D.D.C. 2002). Thus, the inquiry ends without any discussion of the public's interest in disclosure because exemption 7(F) is an "absolute ban." *Id.* Moreover, courts generally give deference to agency declarations establishing the risks of disclosure. *Gonzalez v. U.S. Customs & Immig. Serv.*, 475 F. Supp. 3d 334, 353 (S.D.N.Y. 2020); *Pinson v. Dep't of Just.*, 199 F. Supp. 3d 203, 216–17 (D.D.C. 2016).

The EID contains sensitive data about individuals that, if exposed, presents a variety of safety concerns for those who could be reidentified. The EID "the EID captures and holds information designated with a High FIPS categorization—the highest sensitivity level—described as information related to investigations, law enforcement, and special operational activities." Fontaine Decl. ¶ 7. This information includes information, if inaccurate, lost, or modified without authorization, "could reasonably be expected to result in a loss of life." *Id.*

Here, as with the privacy interests described above, several groups of individuals who are re-identified through EID data could reasonably face several grave threats to their life and physical safety. These risks are real and could easily materialize if re-identification is achieved because "low-cost data broker sites" can provide "other personal information, including the person's phone number, current and previous home addresses, usernames, email, social media accounts, and the names and contact information of their family members." Lynch Decl. ¶ 46. Using this information, "a motivated individual could use this information . . . to . . . execute attacks." *Id.* Four groups of individuals highlight—but by no means exhaustively represent—the risks to life and physical safety presented by disclosure here.

First, focusing in on the migrants whose records Plaintiffs seek, there are a variety of risks to the safety of those who are the subject of the records. Some records involve migrants with credible fear cases where there is a significant possibility that a migrant facing removal has been persecution or has a well-founded fear of persecution if returned to their country or where it is more likely than not that they would be subject to torture if returned. Lynch Decl. ¶ 17. Additionally, other records reveal, special but standardized "vulnerability codes" that provide information regarding whether "migrant is seriously mentally ill, a victim of sexual abuse or a violent crime, disabled, at risk based on sexual orientation/gender, or otherwise exceptionally vulnerable." *Id.* Notably, if the individuals' identities can be tied to their credible fear cases or their vulnerability codes, then the individuals could be subjected to "discrimination, exploitation, and potentially life-threatening persecution." *Id.* The risks presented to these individuals and their families include "kidnapping, assassination, physical and psychological torture" against either the migrant or the migrant's family members. *Id.*, ¶ 54.

Second, some records Plaintiffs seek pertain to "children's cases as young as newborns." Lynch Decl. ¶¶ 62, 16. Records pertaining to minors could be created for a variety of sensitive reasons: "[c]ases may involve minors charged with crimes or affiliated with gangs, including minors who have fled cartels and have credible fears of retaliation." *Id.*, ¶ 18. These records can provide information regarding "whether the child is separated from family, entered the United States as an unaccompanied minor, and where the child resides." *Id.* Risks posed to minors include "abuse and exploitation" of unaccompanied minors, attacks on minors "fleeing gangs and cartels" (either by the gangs, cartels, or their rivals), and "sexual abuse and trafficking both during and after migration." *Id.*, ¶ 62.

Third, a diverse set of groups run a diverse set of risks based on unique circumstances. For example, members of the LGBT community who are re-identified and at the same time associated with their LGBT identity may suffer persecution, "social exclusion, harassment, deprivation of economic opportunities, and acts of violence." Lynch Decl. ¶ 54. Individuals with "disabilities or mental health conditions" revealed by the records "could face discrimination, social exclusion, harassment, and online bullying." *Id.* Individuals who have been associated with "abortional acts" run the risk of being "targeted by politically motivated actors, harassed, and subject[ed] to physical and psychological harms." *Id.*

Fourth, disclosure of EID data pertaining to witnesses to crimes would involve highly sensitive personal information, including information that describes the witness and "whether the witness has information that may be relevant to federal investigations or if they may be called upon to testify in official court proceedings." Lynch Decl. ¶ 23. Witnesses to incidents "are exceptionally vulnerable to threats of retaliation" by "highly organized and violent cartels, human traffickers, and smugglers." *Id.*, ¶ 55.

More broadly, the public at large could be presented with threats to life and physical safety if, because of disclosure, the EID becomes subject to a cyberattack that locked ICE and its law enforcement partners out of the EID. In that scenario, law enforcement officers would be impeded in their ability to "identify, arrest and detain individuals who are terrorists, national security threats [and] threats to public safety." Fontaine Decl. ¶ 20. Relatedly, law enforcement personnel "would be unable to use the [EID] to determine an encountered individual's criminal history, fingerprints and other biometrics, and other factors essential to understanding the threat that individual may represent to the public," which in turn "could reasonably result in ICE officers being required to release dangerous individuals who would otherwise be arrested." *Id.*

B. The EID Data Is Exempt From Disclosure Under FOIA Exemption 6 Because It Contains Sensitive Information Linked To An Individual.

FOIA does not require an agency to disclose "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6); *U.S. Dep't of State v. Wa. Post Co.*, 456 U.S. 595 (1982); *Cook v. Nat'l Archives & Recs. Admin.*, 758 F.3d 168, 174 (2d Cir. 2014); *Burton v. Wolf*, 803 F. App'x 120, 121 (9th Cir. 2020); *Wood v. Fed'l Bureau of Investig.*, 432 F.3d 78, 86–87 (2d Cir. 2005). Here, while the EID is not structured on a person-by-person basis, Plaintiffs seek to obtain EID information for the purpose of tracking data about individual people insofar as Plaintiffs seek "relational information" and all datapoints "directly or indirectly linked" to a person. Katz Decl. Exh. **"C"**. Thus, Plaintiffs seek data pertaining to individuals that would constitute "similar files" that would constitute a clearly unwarranted invasion of personal privacy. *Cook*, 758 F.3d at 174.

For example, in *Burton v. Wolf*, 803 F. App'x 120, 121 (9th Cir. 2020), the Court found alien files constituted "similar files" because the files contained "personal identifying information." And, the Second Circuit in *Associated Press v. Department of Defense*, 554 F.3d 274 (2d Cir. 2009), found that records pertaining to detainees constituted "similar files" because the records constituted files about an "individual which can be identified as applying to that individual." Of particular note to this case, the files do not need to be kept as a "file" on an individual in order to qualify for protection. *Cook*, 758 F.3d at 174.

As to the privacy interests that would be invaded, the principles of the analysis from Exemption 7(C) likewise applies to Exemption 6. *Reps. Comm. for Freedom of the Press*, 489 U.S. at 763 (1989). Further, for the same reasons explained in Point II(A)(ii), disclosing the EID data would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). ICE adopts the analysis performed there as if fully set forth here.

C. EID Datapoints Include A Multitude Of Data That Is Protected From Disclosure By Other Statutes and Regulations, Rendering It Exempt Under Exemption 3

FOIA does not require an agency to comply with FOIA's disclosure obligations at the expense of violating another statute. 5 U.S.C. § 552(b)(3).[9] But that is exactly what Plaintiffs seek to do here. Indeed, EID includes a large variety of fields that implicate ICE's various duties to protect sensitive and/or private information. There are two paths to invoking exemption 3. First, an agency can show a qualifying statute "requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue. 5 U.S.C. § 552(b)(3)(A)(i). Second, an agency can show a qualifying statute "establishes particular criteria for withholding or refers to particular types of matters to be withheld," which are subject to the request. 5 U.S.C. § 552(b)(3)(A)(ii).

Based on a preliminary review of the EID datapoints, the EID data could implicate any number of statutes that prohibit disclosures. Indeed, the production of EID data—which contains thousands of datapoints—will involve analyzing each datapoint at the outset to determine whether it would categorically include information prohibited from disclosure by more than a dozen different statutes with different scopes, including but not limited to the following statutes:

- 8 U.S.C. § 1367(a)(2), which provides, "in no case may . . . any other official or employee . . . the Department of Homeland Security . . . permit use by or disclosure to anyone (other than a sworn officer or employee of the Department, or bureau or agency thereof, for legitimate Department . . . purposes) of any information which relates to an alien who is the beneficiary of an application for relief under paragraph (15)(T), (15)(U), or (51) of section 101(a) of the Immigration and Nationality Act

[9] For statutes enacted after the OPEN FOIA Act of 2009, the qualifying statute must specifically state it is creating an exemption from FOIA disclosure. However, none of the statutes listed here were enacted after the OPEN FOIA Act of 2009.

or section 240A(b)(2) of such Act."[10] 8 C.F.R § 1208.6 prohibits disclosure of information contained in or pertaining to any application for refugee status, asylum, withholding or removal or protection under the Convention Against Torture's implementing legislation, including records pertaining to any credible fear determination or reasonable fear determination, without consent of the applicant. Lynch Decl. ¶¶ 15, 52. Also, witnesses involved in criminal incidents, or testifying in cases against cartels, human traffickers, and smugglers. *Id.*, ¶¶ 21, 53.

- 8 U.S.C. § 1202(f), which states, "records of the Department of State and of diplomatic and consular offices of the United States pertaining to the issuance or refusal of visas or permits to enter the United States shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States."
- 10 U.S.C. § 130b, which prohibits disclosure of information pertaining to "any member of the armed forces assigned to an overseas unit, a sensitive unit, or a routinely deployable unit" as well as "any employee of the Department of Defense or of the Coast Guard whose duty station is with any such unit."
- 18 U.S.C. § 3509(d), which pertains to protecting child victims of crimes from having their identities disclosed.

---

[10] Section 1367 protects *any* information relating to non-citizens, and their beneficiaries, who are seeking or have been approved for immigrant status as (1) battered spouses, children and parents under provisions of the Violence Against Women Act (VAWA); (2) victims of a severe form of human trafficking who generally are cooperating with law enforcement authorities; or (3) victims who have suffered substantial physical or mental abuse and are cooperating with law enforcement authorities.

- 26 U.S.C. §§ 6103, 6105, which prohibits a government employee from disclosing "any [tax] return or return information obtained by him in any manner in connection with his service as such an officer or an employee or otherwise or under the provisions of this section."
- 49 U.S.C. § 114(r), which empowered the Administrator of the Transportation Security Administration to "prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security under authority of the Aviation and Transportation Security Act (Public Law 107-71)" under certain circumstances.
- Fed. R. Crim. P. 6(e), which pertains to the secrecy of grand jury proceedings.
- 18 U.S.C. § 2510, *et seq.*, and 18 U.S.C. § 3123(d), which pertain to law enforcement activities that include wire taps and pen registers.
- 50 U.S.C. § 3024(i)(1), which pertains to protecting "intelligence sources and methods from unauthorized disclosure." *See also* 50 U.S.C. § 3507; 50 U.S.C. § 403-1(i)(1) (National Security Act of 1947).

D. The Exempt Data In The EID Is Not Reasonably Segregable From The Non-Exempt Data.

Where certain FOIA exemptions apply, the next question becomes whether the exempt records can be reasonably segregated from the non-exempt data. *Sorin v. Dep't of Just.*, 758 F. App'x 28, 33 (2d Cir. 2018); *Lead Indus. Ass'n v. Occupational Safety & Health Admin.*, 610 F.2d 70, 86 (2d Cir. 1979). As relevant here, data is not reasonably segregable where (1) nonexempt information is "inextricably intertwined" with exempt information, or (2) the agency would be required to create new records to comply with the FOIA request. *Mead Data Cent., Inc. v. Dep't of the Air Force*, 566 F.2d 242, 260 (D.C. Cir. 1977) ("inextricably intertwined"); *Fischer v. Dep't*

of Just., 723 F. Supp. 2d 104, 115 (D.D.C. 2010) (same); *Cole v. Copan*, No. 19-1182, 2020 WL 7042814, at *7 (D.D.C. Nov. 30, 2020) (new record).

Courts take a practical approach to the reasonable segregation analysis. To that end, courts consider whether "excision of exempt information would impose significant costs on the agency," including the volume of the data that would need to be segregated. *Durrani v. Dep't of Just.*, 607 F. Supp. 2d 77, 88 (D.D.C. 2009); *FlightSafety Servs. Corp. v. Dep't of Labor*, 326 F.3d 607, 613 (5th Cir. 2003); *Solar Sources*, *Inc. v. United States*, 142 F.3d 1033, 1039 (7th Cir. 1998). Additionally, courts consider whether an agency has the technical capability to reasonably segregate the exempt data from the non-exempt data. *Milton v. Dep't of Just.*, 842 F. Supp. 2d 257, 259–61 (D.D.C. 2012).

Here, ICE cannot achieve reasonable segregation merely by redacting or excluding certain fields from the search or production. The EID contains diverse types of information, which can present a detailed picture of a person even after ICE removes direct identifying information. Lynch Decl. ¶¶ 5–9. The EID contains "approximately 12,000 data fields directly or indirectly linked to a migrant's case, including personal information (PI), sensitive personal information (SPI), and demographically identifiable information (DII)." *Id.*, ¶ 5. And "[a]dvanced analytic techniques allow the technically savvy to identify individuals even when direct identifiers have been stripped." *Id.*, ¶ 30.

As explained above, mitigating the risk of re-identification is not a simple process of removing direct identifiers or using substitute identifiers. Lynch Decl. ¶¶ 6, 10. Indeed, Plaintiffs' request that ICE preserve "relational information" (as they define that term) undermines any purported privacy benefits afforded by substitute identifiers. *Id.* By presenting the data as related, ICE would be connecting various data that would only serve to make re-identification easier. *Id.*

In a chilling experiment, "ICE cybersecurity personnel were able to re-identify individuals from sample EID records **stripped of full names and other direct identifiers** simply by searching local city and state online public arrest records" based on data within EID. Lynch Decl. ¶ 44. Moreover, even after more information was removed regarding detention dates, "dates could be deduced based on date and time stamps that are automatically generated when detention records are first created." *Id.*, ¶ 45.

The risks of reidentification of individuals from pseudonymized EID data—which undermines the protection of the information—are grave, tangible, and ever-increasing. Lynch Decl. ¶¶ 30, 51. Bad actors, all have interests in identifying—and potentially retaliating or exploiting—individuals whose information is contained within the EID. *Id.*, ¶ 52. These bad actors have a variety of reasons to exploit EID data, including retaliation against informants and cooperators, punishment for failed criminal operations, identification of victims (such as trafficking victims) and potential victims, or as a means to weaken rivals. *Id.*, ¶ 53. These groups may seek out specific people through information in EID, including "an individual's gang affiliation, gang role, gang tattoos, criminal histories, and detailed information about criminal incidents and property seized by law enforcement." *Id.*, ¶ 52. Moreover, for those being detained, bad actors could find out "where migrants are located, whether in jail, prison, detention facilities, . . . or otherwise," which would give those bad actors a place to lie in wait for their victims to emerge. *Id.*

These risks are exacerbated by the breadth of Plaintiffs' request: "[t]he scale, scope, and historical nature of the requested EID data significantly enhance the feasibility of developing highly accurate . . . algorithms." Lynch Decl. ¶ 32. These risks are also exacerbated by the availability of publicly available information, which can be cross-referenced against EID data to

increase the risk of re-identification. *Id.*, ¶¶ 43, 45.

The risk of re-identification can only be mitigated by *anonymizing* the data, which is a complex process that involves ensuring that the datapoints—individually and as a whole—cannot be used as indirect identifiers to reconstruct the identity of the subject of the information. Lynch Decl. ¶ 13. "Indirect identifiers are PI that can reveal a person's identity in combination with other data." *Id.*, ¶ 6. Anonymizing the data would be a laborious process that would require extensive analysis and sophisticated testing. *Id.*, ¶ 13. Further complicating the matter, ICE would need to account for the potential that future technology would make a dataset that has been currently anonymized subject to further re-identification. *Id*. For these reasons, to anonymize the data would not be feasible given that Plaintiffs seek to have ICE use substitute identifiers and "relational information." *Id.*

Whether information qualifies as an indirect identifier of a person depends on several factors, most notably what other data is available. Examples of indirect identifiers often seem innocuous—at least until combined with other data—and include gender, birth year, occupation, or country of origin. Lynch Decl. ¶ 6. On the one hand, facially sensitive information is present throughout the EID, including whether an individual is transgender or whether the individual has survived a rape. *Id.*, ¶ 7. On the other hand, even seemingly inert demographic or administrative data (such as location, time, and date data) can present threats to safety. *Id.*, ¶¶ 8, 18–20. Location data particularly stands out as an example. Location data can be used to reconstruct individuals' movements. *Id.*, ¶ 19. And, as another example, location data can be used to determine where people are housed within federal facilities. *Id.*, ¶¶ 19–20; see also *id.*, ¶ 19 ("The EID also stores granular information regarding vehicles and property seized in criminal incidents.").

Moreover, the segregation analysis could reasonably change based on the specific data at issue. Notably, while some data pertains to an individual migrant, other data pertains to their relatives, associates, and the professionals who engage in a migrant's case over time. The data available on each of these groups would need to be separately analyzed to determine how much data has been collected and how much data would need to be stripped away to ensure anonymization.

CONCLUSION

For these reasons, U.S. Immigration and Customs Enforcement respectfully requests that this Court enter an Order granting summary judgment and, accordingly, dismissing this action as against U.S. Immigration and Customs Enforcement along with such further relief as this Court deems fair, just, and equitable.

Dated: October 1, 2024

CARLA B. FREEDMAN
United States Attorney

By: /s/
David M. Katz
Assistant United States Attorney
Bar Roll No. 700065